Dr.WEB®
Agent
for Novell NetWare

Defend what you create

User Manual

© 2004-2012 Doctor Web. All rights reserved.

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

TRADEMARKS
Dr.Web, the Dr.WEB logo, SpIDer Mail, SpIDer Guard, CureIt!, the Dr.WEB INSIDE logo are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER
In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web Enterprise Agent for Novell® NetWare®
Version 6.0
User Manual
20.04.2012

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web® information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Chapter 1. Welcome to Dr.Web® Enterprise Security Suite 6

1.1. Conventions and Abbreviations 6

1.2. Dr.Web Enterprise Security Suite Anti-Virus 7

Chapter 2. Dr.Web Enterprise Agent for Novell® NetWare® 8

2.1. Main Functions and Parameters of the Dr.Web Agent 8

2.2. System Requirements 9

2.3. Installing and Removing Dr.Web Agents 9

2.4. Updating Dr.Web Agent 10

Chapter 3. Configuring Integration with Dr.Web Enterprise Security Suite 12

3.1. Configuring Dr.Web Agent 12

3.2. Registering with Enterprise Security Suite Server 13

3.3. Launching Dr.Web Anti-Virus for Novell® NetWare® 14

3.4. Configuring via the Dr.Web Control Center 15

Chapter 4. Dr.Web Agent for Novell® NetWare® Settings 16

4.1. [Logging] Section 16

4.2. [Agent] Section 17

4.3. [Server] Section 18

4.4. [EnterpriseMode] Section 18

4.5. [StandaloneMode] Section 19

4.6. [Update] Section 20

Appendix A. Technical Support 21

Chapter 1. Welcome to Dr.Web® Enterprise Security Suite

1.1. Conventions and Abbreviations

The following conventions are used in the Manual:

Symbol	Comment
Note, that	Marks important notes or instructions.
Warning	Warns about possible errors.
Dr.Web Agent	Names of **Dr.Web** products and components.
Anti-virus network	A term in the position of a definition or a link to a definition.
<IP-address>	Placeholders.
Cancel	Names of buttons, windows, menu items and other user interface elements.
CTRL	Keyboard keys names.
`C:\Windows\`	Names of files and folders, code examples, input to the command line and application output.
Chapter 3	Cross-references or Internal Hyperlinks to web pages.

The following abbreviations will be used in the Manual without further interpretation:

- OS — operating system,
- PC — personal computer.

1.2. Dr.Web Enterprise Security Suite Anti-Virus

Dr.Web Enterprise Security Suite is designed to organize and control integrated, complex and reliable anti-virus protection of computers of a company.

Protected computers are united in an anti-virus network, which is managed by the administrator through the **Enterprise Server**. The anti-virus protection of company's employees computers is automated and administered centrally, which provides for a reliable safety level, while user interference is minimal.

Dr.Web Enterprise Security Suite provides for

- centralized (without user intervention) installation of the anti-virus packages on computers,
- centralized setup of anti-virus packages on protected computers,
- centralized virus databases and program files updates on protected computers,
- monitoring of virus events and the state of anti-virus packages and OS's on all protected computers.

Dr.Web Agents are installed on protected computers. These components provide for computer protection and connection with the **Enterprise Server**, through which anti-virus programs and their components are updated and set up in general.

Chapter 2. Dr.Web Enterprise Agent for Novell® NetWare®

2.1. Main Functions and Parameters of the Dr.Web Agent

Anti-virus protection of servers operated by Novell NetWare is provided by means of components included in the anti-virus package of **Dr.Web Anti-virus for Novell NetWare**.

Dr.Web Enterprise Agent for Novell® NetWare® (hereinafter - **Dr.Web Agent**) implements computer's protection management and connection to the **Enterprise Server**.

Dr.Web Agent can operate in one of the following modes:

- *Standalone*.
- *Enterprise*.

Actual functions performed by **Dr.Web Agent** depend on its operation mode.

In the Enterprise mode, the Dr.Web Agent serves the following functions:

- Provides a connection with the **Enterprise Server**.
- Updates and sets up the anti-virus package components.
- Defines operation policy of anti-virus packages according to current license.
- Sends the results of scans and virus events statistics to the anti-virus **Server**.

In the *Standalone* mode, the **Dr.Web Agent** do not establish connection with the **Enterprise Server**.

When **Dr.Web anti-virus solutions** are integrated with **Dr. Web Enterprise Security Suite**, users must have appropriate

permissions to configure anti-virus packages on their computers. For details on permission restriction, see **Dr.Web Enterprise Security Suite Administrator Guide**.

2.2. System Requirements

Do not install other anti-virus programs, including other **Dr.Web** programs, on computers with an installed anti-virus **Agent**.

Installing two anti-virus programs on one computer may lead to system crash and loss of important data.

Dr.Web Agent is a NetWare Loadable Module® (NLM®) that supports operation on servers running under Novell NetWare 4.11 SP9, 4.2, 5.1, 6.0, or 6.5 operating system.

For integration with **Dr.Web Enterprise Security Suite** anti-virus network, it is required:

- **Dr.Web Anti-virus for Novell NetWare** of **5.0** version and later.
- **Dr.Web Agent for Novell NetWare** of **6.0** version and later.
- **Dr.Web Enterprise Security Suite** of **6.0** version and later.

2.3. Installing and Removing Dr.Web Agents

Dr.Web Agent Installation

To install the Dr.Web Agent:

1. Download the **Agent** distribution kit from the http://www.drweb.com/ **Doctor Web** web site.
2. Unpack the **Agent** distribution archive into the installation directory of the **Dr.Web Anti-virus for Novell NetWare**. The **Agent** configuration file must be edited manually to configure the **Enterprise** mode (see Configuring Dr.Web Agent).

3. Configure integration of **Dr.Web Anti-virus for Novell NetWare** with **Dr.Web Enterprise Security Suite** (for more information, see Chapter 3. Configuring Integration with Enterprise Security Suite).

Dr.Web Agent Removing

After removing anti-virus software, remote computer will not be protected from security threats.

1. From the **Dr.Web Anti-virus for Novell NetWare** Console, stop the `drwebnw` module.
2. Run the following command to unload **Dr.Web Agent**:
   `unload nwesag`
3. Delete the `nwesag.nlm` **Agent** module from the installation folder of the **Dr.Web Anti-virus for Novell NetWare** at the Novell NetWare server.

   Also delete the following files, which are used by the **Agent**:

   - agent.pwd password file,
   - agent.cfg **Agent** configuration file,
   - agent.log **Agent** log file,
   - drwcsd.pub public key file, that is used for connecting to the **Enterprise Server**,
   - agent.reg file, that contains the list of installed updates,
   - cache temporary directory where the **Agent** stores downloaded update files.

2.4. Updating Dr.Web Agent

To update Dr.Web Agent:

1. Download the **Agent** distribution archive to the Novell NetWare server with installed **Dr.Web Anti-virus for Novell NetWare** antivirus package.
2. From the **Dr.Web Anti-virus for Novell NetWare** Console, stop the `drwebnw` module.

3. Run the following command to unload **Dr.Web Agent**:
   ```
   unload nwesag
   ```
4. Delete the `nwesag.nlm` **Agent** module from the installation folder of the **Dr.Web Anti-virus for Novell NetWare** at the Novell NetWare server.
5. Unpack the **Agent** distribution archive into the installation folder of the **Dr.Web Anti-virus for Novell NetWare**.
6. Run the following command from the server or a remote console to start **Dr.Web Agent**:
   ```
   load [ <full_path>] nwesag
   ```
   where *<full_path>* is the path to the **Agent** installation folder on the server. If the directory is located according to the path in the server configuration files (`autoexec.ncf`), you do not need to enter the path.

For more information about additional update parameters, see the [Update] section.

Chapter 3. Configuring Integration with Dr.Web Enterprise Security Suite

If the **Dr.Web for Novell NetWare Anti-virus** is already installed on Novel NetWare server, it is possible to connect this server to the **Dr. Web Enterprise Security Suite** anti-virus network.

To configure integration with Dr.Web Enterprise Security Suite

1. Install and configure **Dr.Web Anti-virus for Novell NetWare.** For details, refer to **Dr.Web Anti-virus for Novell NetWare User Manual**.
2. Install the **Dr.Web Agent**.
3. Configure the **Dr.Web Agent** for operating in **Enterprise** mode.
4. Launch the **Dr.Web Agent**.
5. Register the remote computer at the **Enterprise Server**.
6. Configure settings of **Dr.Web** anti-virus components for Novell NetWare via the **Dr.Web Control Center**.

3.1. Configuring Dr.Web Agent

After unpacking the **Agent** distribution archive into the **Dr.Web Anti-virus for Novell NetWare** installation directory, its configuration file must be edited manually to configure the **Enterprise** mode.

Configuring Enterprise Mode

You must unload **Dr.Web Agent** before editing the configuration file. Otherwise your changes will be lost, since the program overwrites this file after each session with recently used settings.

To configure the Enterprise mode of the Agent:

1. Open the **Agent** configuration file for editing in a text editor. By default, the configuration file is located in the installation folder and is called `agent.cfg`.
2. In the `[EnterpriseMode]` section, set the following parameters:
   - `PublicKeyFile` - path to the public key file for access the **Enterprise Server**.
   - `ServerHost` - the **Enterprise Server** IP address.
   - `ServerPort` - the **Enterprise Server** port number (by default, 2193).
3. Copy the public key file from the **Enterprise Server** to the directory on the remote computer that you specified in the `PublicKeyFile` parameter at the previous step.
4. Save changes in the configuration file.

3.2. Registering with Enterprise Security Suite Server

Registration

When the **Agent** is launched in the **Enterprise** mode, it must accomplish the registration at the **Enterprise Server** and get account details (station ID and password).

Registration at the **Enterprise Server** can be provided by one of the following ways:

1. If **Enterprise Security Suite Server** is set to operate in Approve access manually mode, then registration of the new workstation must be confirmed by an anti-virus network administrator via **Dr.Web Control Center**.
2. If **Enterprise Security Suite Server** is set to operate in Approve access automatically mode, station will be registered automatically at the **Enterprise Server** at first access.

Accessing modes configuration is described in the **6.1** chapter of the **Dr.Web Enterprise Security Suite Administrator manual**.

After registration, the **Agent** records the hash of station ID and password to the password file.

Password File

Connection between **Enterprise Server** and **Agents** running on remote computers is carried out using special password files that store information on remote computers, identifiers and connection passwords. Data from this file is used every time **Agents** connect to **Enterprise Servers**.

For remote computers running under Novell NetWare operating systems, the path to the password file should be set in the `PasswordFile` parameter in the `[EnterpriseMode]` section of the **Agent** configuration file (by default, `agent.pwd` that is stored at the directory, specified in the agent.cfg).

According to the specified path, the **Agent** creates the password file at first connection to the **Enterprise Server**.

If the password file has been deleted, repeated registration request will be made to **Enterprise Server** when **Agent** launches next time.

3.3. Launching Dr.Web Anti-Virus for Novell® NetWare®

After you configured integration with **Enterprise Server**, start the **Dr.Web Anti-virus for Novell NetWare**.

To launch the system:

1. Run the following command from the server or a remote console to start **Dr.Web Agent**:
   `load [` *<full_path>*`] nwesag`
   where *<full_path>* is the path to the **Agent** installation folder on

the server. If the directory is located according to the path in the server configuration files, you do not need to enter the path.

2. **Agent** loads necessary modules automatically.

If you have not installed latest updates and patches for Novell NetWare, the module may not load. In this case, the following message displays:

```
...Module nwesag.nlm cannot be loaded until CLIBAUX loaded...
```

You can find necessary updates at http://support.novell.com/patches.html.

If **Dr.Web Anti-virus for Novell NetWare** is configured to provide e-mail notifications, the `tcpip.nlm` module is to be loaded on the server, which requires the TCP/IP protocol to be configured. Otherwise, the following error message displays at startup:

```
TCPIP.NLM not loaded (error <error number>). Some additional features are not available.
```

3.4. Configuring via the Dr.Web Control Center

Dr.Web Anti-virus for Novell NetWare package includes default configuration files for supported **Dr.Web** anti-virus components.

When you configure anti-virus components via the **Dr.Web Control Center**, values for the corresponding parameters are changed at the **Enterprise Server** and transferred to the **Agent** every time when **Dr.Web** anti-virus components start on remote computers.

For details on **Dr.Web Anti-virus for Novell NetWare** parameters, refer to Chapter 4 of **Dr.Web Anti-virus for Novell NetWare User Manual**.

For details on managing remote anti-virus solutions via the **Dr.Web Control Center**, refer to **Dr.Web Enterprise Security Suite Administrator Guide**.

Chapter 4. Dr.Web Agent for Novell® NetWare® Settings

Dr.Web Agent settings can be configured via the `agent.cfg` configuration file. This file is located in the same directory as the `drwebnw.nlm` and `nwesag.nlm` program modules. If the configuration file is missing, the program will use the default settings. In any case all settings of the last session are saved to the configuration file automatically.

You must unload **Dr.Web Agent** before editing the configuration file. Otherwise your changes will be lost, since the program overwrites this file after each session with recently used settings.

Agent configuration file contains the following sections:

- [Logging] - logging options for registration of virus events on remote computer.
- [Agent] - **Agent** general settings.
- [Server] - **Enterprise Server** connection settings.
- [EnterpriseMode] - settings of the **Agent** operation within the **Dr.Web Enterprise Security Suite** anti-virus network.
- [StandaloneMode] - settings of the **Agent** operation in the *Standalone* mode.
- [Update] - additional update parameters.

4.1. [Logging] Section

In the `[Logging]` section, logging options on virus events at the remote computer are set:

Parameter	Description
Level	Sets one of the following log detail level:

Parameter	Description
	• **Debug** – log debugging events (maximum detail); • **Info** – log information messages; • **Alert** – log major informational messages; • **Error** – log operation errors; • **Quiet** – inform on most severe errors only (minimum detail).
IPCLevel	Sets one of the log detail level for the interprocess communication module. Details levels are similar to levels of the `Level` parameter.
SyslogFacility	Type of device for generation of event notifications, if the system log service is enabled
FileName	Name for the log file (`agent.log`). You may specify `syslog` as a value, the report will be logged by means of `syslogd` system service.

4.2. [Agent] Section

In the `[Agent]` section, general options of the **Agent** are set:

Parameter	Description
MetaConfigDir	Path to the directory with meta-configuration file of the **Agent**
UseMonitor	Defines, if active scan processes are monitored. `yes` and `no` are allowed.
MonitorAddress	Socket for monitoring system
MonitorResponseTime	Maximal response time for monitoring system
PidFile	Path to PID file, which has been written during **Agent** launch

4.3. [Server] Section

In the `[Server]` section, parameters for communication with the **Enterprise Server** are set:

Parameter	Description
Timeout	Period for **Agent** to wait for connection from the **Enterprise Security Suite Server**
Address	Socket for connection between **Agent** and the **Server**
Threads	Number of synchronous threads for connection with the **Server**

4.4. [EnterpriseMode] Section

In the `[EnterpriseMode]` section, parameters for operation of the **Agent** in **Enterprise** mode are set:

Parameter	Description
UseEnterpriseMode	Defines, if the **Agent** operates in the **Enterprise** mode. Allowed values: `yes` - the **Enterprise** mode is enabled, `no` - operation is in the **Standalone** mode
PasswordFile	Location of the password file used when **Agent** connects to the **Enterprise Server**
ComputerName	**Agent for NetWare** name. If not set, the host name is used
VirusbaseDir	Location of **Dr.Web virus databases**
PublicKeyFile	Location of the `drwcsd.pub` - the **Dr.Web Agent** public key file
ServerHost	The **Enterprise Server** IP address
ServerPort	The **Enterprise Server** port
CryptTraffic	Encryption settings for traffic between **Agent for NetWare** and **Enterprise Server**: • **Yes** – enables obligatory traffic encryption for all components;

Parameter	Description
	• **Possible** – instructs to encrypt traffic with those components whose settings do not prohibit it; • **No** – encryption is not supported
CompressTraffic	Compression settings for traffic between **Agent for NetWare** and **Enterprise Server**: • **Yes** – enables obligatory traffic compression for all components; • **Possible** – instructs to compress traffic with those components whose settings do not prohibit it; • **No** – compression is not supported

4.5. [StandaloneMode] Section

In the `[StandaloneMode]` section, options of the **Standalone** mode of the **Agent** not connected to the **Enterprise Server** are set:

Parameter	Description
StatisticsServer	IP address or DNS name of virus statistics server of **Doctor Web** company
UrlStatisticsServer	IP address or DNS name of server of collecting statistics on harmful web sites URL
StatisticsUpdatePeriod	Period of updating statistics by the **Agent** in minutes (not less than 6 minutes)
StatisticsProxy	IP address or DNS name of http proxy server for sending the virus statistics
StatisticsProxyAuth	Login and password for authentication on proxy server
UUID	Should be set only if personal UUID is used for accessing to statistics server
LicenseFile	Path to local licence key file. You can specify several key files
ProtectedEmails	List of protected e-mails. You can specify addresses directly or via the file or ldap

4.6. [Update] Section

In the `[ Update]` section, additional update parameters for the remote computer are set:

Parameter	Description
CacheDir	A temporary directory where the **Agent** stores downloaded update files (`cache`)
RegFile	A file where the **Agent** registers installed updates (`agent. reg`)
Timeout	Maximal allowed time in seconds for receiving updates by the **Agent**
RootDir	Root directory

Dr.Web software updates are loaded and installed automatically as they become available. In critical situations you can manually update the software components.

For details on the update procedure, refer to **Dr.Web Anti-virus for Novell NetWare User Guide**.

Appendix A. Technical Support

Support is available to customers who have purchased a commercial version of **Dr.Web** products. Visit **Doctor Web Technical Support** website at http://support.drweb.com/.

If you encounter any issues installing or using company products, take advantage of the following **Doctor Web** support options:

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Look for the answer in Dr.Web knowledge database at http://wiki.drweb.com/
- Browse Dr.Web official forum at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from **Doctor Web Technical Support** by filling in the web-from in the corresponding section of the support site at http://support.drweb.com/.

For regional office information, visit the **official Doctor Web website** at http://company.drweb.com/contacts/moscow.

© 2004-2012 Doctor Web